1

DERECHOS HUMANOS Y SEGURIDAD DIGITAL: UNA PAREJA PERFECTA

Aportes de la sociedad civil hacia políticas nacionales de seguridad digital que respeten y protejan los derechos humanos

Maricarmen Sequera, Amalia Toledo & Leandro Ucciferri

Enero 2018

Esta publicación es el primer documento de la serie *Análisis de políticas sobre ciberseguridad y derechos humanos en Latinoamérica,* que desarrollan en conjunto las organizaciones TEDIC de Paraguay, la Asociación por los Derechos Civiles (ADC) de Argentina y la Fundación Karisma de Colombia. Ha sido posible gracias al apoyo y financiación de Privacy International y Ford Foundation.

Autores:
Maricarmen Sequera, TEDIC,
Leandro Ucciferri, ADC
Amalia Toledo, Fundación Karisma

Revisión:
Luis Pablo Alonzo
Carolina Botero

Colaboración:
Francisco Vera
Lucy Purdon

Diseño editorial:
Diantres

Enero 2018









TABLA DE CONTENIDOS

INTRODUCCIÓN

La dependencia de las tecnologías de la información y las comunicaciones interconectadas globalmente ha puesto en el centro de la discusión la necesidad de trabajar en políticas y/o estrategias nacionales de seguridad digital. Esta necesidad es alimentada por el aumento de incidentes y ataques digitales con potenciales consecuencias catastróficas para la protección de la seguridad de la información, por tanto, de las personas. De acuerdo a información de la Unión Internacional de Telecomunicaciones (UIT), tan solo 76 de sus 193 Estados miembros cuentan con algún tipo de política, estrategia o norma nacional de seguridad digital.[1] De estos, solo 6 de 33 países pertenecientes a la región de Latinoamérica y el Caribe cuenta con una política o estrategia al respecto.

Siendo la seguridad digital una discusión cada vez más crítica, hay que reconocer que la sociedad civil y los grupos de interés público no han sido suficientemente considerados, algo que desequilibra el debate y lo ubica en un tema enfocado en los sistemas o vagos conceptos de seguridad nacional, en lugar de las personas.

Sin embargo, la seguridad digital está intrínsecamente relacionada con las personas, pues la forma en cómo se definen e implementan las políticas de regulación del comportamiento en línea y la seguridad de la información tienen profundas implicaciones para los derechos humanos, en especial la privacidad, la libertad de expresión o la libre asociación.

Cómo se entiende la seguridad digital es una pregunta central para la elaboración de políticas, pero difícil de responder, pues existen numerosas definiciones. A eso se suma la dificultad de encontrar una definición que incluya compromisos claros por el respeto a los derechos humanos.[2] Esto se complejiza aún más cuando se introducen otros conceptos que agregan más confusión como cibercrimen, ciberguerra y ciberdefensa.

---

1 ITU. (2017). ***National Strategies.*** Disponible en http://www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies.aspx

2 New America Foundation. (s.f.). *Global Cyber Definitions Database*. Disponible en http://cyberdefinitions.newamerica.org/

Sin embargo, como se ha planteado en múltiples foros, "la seguridad digital y los derechos humanos son complementarios, se refuerzan mutuamente y son interdependientes".[3] Por lo tanto, es imperativo reconocer que el núcleo de la seguridad digital debe estar en la protección de las personas y, consecuentemente, de los derechos humanos. En tal sentido, la definición que guía este informe es la desarrollada por el grupo de trabajo 1 "Una Internet libre y segura"[4] de la *Freedom Online Coalition*, pues entendemos es la más respetuosa con los derechos humanos:

> La ciberseguridad es la preservación, a través de políticas, tecnología y educación, de la disponibilidad, confidencialidad e integridad de la información y su infraestructura subyacente a fin de mejorar la seguridad de las personas tanto online como *offline*.[5]

Esta definición reconoce la importancia de respetar los derechos humanos tanto en línea como fuera de línea. Además, considera el papel de la innovación tecnológica como motor para promover la libre circulación de información en medios digitales. De esta forma, refuerza esa relación entre seguridad digital y derechos humanos para promover la libertad y la seguridad.

Con el ánimo de aportar a los esfuerzos de la Organización de Estados Americanos (OEA) de acompañamiento a los Estados de la región en la elaboración de políticas o estrategias nacionales de seguridad digital, un grupo de organizaciones de la sociedad civil presentamos en 2016 una declaración de principios sobre el tema. El objetivo fue ofrecer unas guías mínimas a tener en cuenta en estos procesos de construcción de políticas o estrategias. En su primer principio y para enmarcar la discusión, el texto de la Declaración propone:

> Alinear cualquier estrategia de seguridad digital con los marcos legales de derechos humanos de cada país, del sistema interamericano y de estándares internacionales como los descritos en los Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones, dando especial relevancia a la protección y garantía al ejercicio de los derechos a la libertad de expresión, a la privacidad y a la libre asociación [...][6]

---

3 FOC-WG1 (s.f.). *An Internet Free and Secure: A Human Rights Approach to Cybersecurity Policy-making.* Disponible en https://freedomonlinecoalition.com/wp-content/uploads/2014/04/FOC-WG1-Narrative-Final-28-April-2016.pdf

4 Freedom Online Coalition. (s.f.). WG 1 – *An Internet Free and Secure*. Disponible en https://freedomonlinecoalition.com/working-groups/working-group-1/

5 FOC-WG1. (2014). *Recommendations for Human Rights Based Approaches to Cybersecurity.* Disponible en https://freedomonlinecoalition.com/wp-content/uploads/2014/04/FOC-WG1-Recommendations-Final-21Sept-2015.pdf

6 *Declaración sobre Seguridad Digital en América Latina.* (2016, 1 de abril). Disponible en https://karisma.org.co/declaracion-sobre-seguridad-digital-en-america-latina/

Estamos convencidos que tal enfoque es fundamental para recordar a las entidades estatales responsables de formulación de políticas públicas que la seguridad digital debe tener en cuenta la seguridad de las personas y los derechos humanos. Por ello, en este informe profundizamos en los principios con explicaciones más amplias y recomendaciones de acciones concretas de pasos a seguir para guiar el desarrollo de políticas o estrategias nacionales de seguridad digital hacia el respeto y la protección de los derechos humanos. A su vez, intentamos ofrecer una visión que ayude a enfrentar los desafíos que los cambios tecnológicos plantean para los Estados y su desarrollo socioeconómico.

DECLARACIÓN CONJUNTA DE SEGURIDAD DIGITAL

Principio 1. Abordar la seguridad digital desde los derechos humanos

Alinear cualquier estrategia de seguridad digital con los marcos legales de derechos humanos de cada país, del sistema interamericano y de estándares internacionales como los descritos en los *Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones*, dando especial relevancia a la protección y garantía al ejercicio de los derechos a la libertad de expresión, a la privacidad y a la libre asociación. Esto incluye mejorar los marcos legales nacionales para garantizar que la vigilancia de las comunicaciones se lleva a cabo de conformidad con las normas de derechos humanos, especialmente con base en los mencionados principios de necesidad y proporcionalidad, y que se adopten y apliquen políticas públicas de protección de datos, particularmente en sus iniciativas y proyectos para compartir información entre países. En ese sentido, es recomendable que el programa de ciberseguridad de la OEA consulte y colabore con otras dependencias de la organización para que sus recomendaciones estén alineadas con los estándares en materia de libertad de expresión y derecho a la intimidad elaborados por la Comisión y la Corte Interamericana de Derechos Humanos y la Relatoría Especial para la Libertad de Expresión de la CIDH.

Principio 2. Sustituir el concepto de ciberseguridad por seguridad digital

Sustituir el concepto de ciberseguridad por el de seguridad digital, que trasciende el ámbito militar y que debe estar centrado conceptualmente en la protección de la ciudadanía, la persona y sus comunidades. La seguridad digital también debe servir para promover el desarrollo económico y social sobre la base de los principios del Estado de derecho y la protección de los derechos fundamentales.

Principio 3. Favorecer prácticas de transparencia y rendición de cuentas

Adoptar instrumentos y mecanismos de transparencia y rendición de cuentas, incluido los planes de Gobierno Abierto, sobre la implementación y desarrollo de las estrategias de seguridad digital en cada país que sean medibles y verificables.

Principio 4. Promover y respetar el uso del cifrado

Reconocer la importancia del cifrado seguro como un elemento de la seguridad digital necesario para la protección de las comunicaciones y de los datos. En consecuencia, es recomendable que los Estados promuevan y respeten su amplio uso y desarrollo por parte de la ciudadanía, las empresas y los gobiernos.

Principio 5. Usar análisis de privacidad por diseño y de impacto en derechos humanos

Usar metodologías de análisis de riesgo como la "privacidad por diseño" y de análisis de impacto sobre los derechos humanos, para fundamentar la formulación e implementación de políticas públicas de seguridad digital basadas en la evidencia.

Principio 6. Desarrollar CSIRT independientes de las fuerzas del orden público

Reconocer que las organizaciones de la sociedad civil tienen debilidades y vulnerabilidades propias que no están siendo atendidas por las actuales estructuras de respuesta a ciberataques (CSIRT). Por tanto, es recomendable desarrollar CSIRT que protejan a la sociedad civil y que no dependan de las fuerzas del orden público, además de que tengan la capacidad para producir datos y respuestas para todos los estamentos de la sociedad en un marco de respeto por los derechos humanos.

Principio 7. Apoyar buenas prácticas de seguridad digital en los sistemas informáticos

Promover e impulsar mejores sistemas informáticos, resilientes y actualizados, que permitan potenciar la seguridad digital. En este sentido, es recomendable que estos sistemas sean auditados de forma pública y constante, permitiendo que su código fuente esté disponible sin trabas legales.

Principio 8. Impulsar la participación multisectorial

Incrementar la colaboración y el intercambio de experiencias entre los países incluyendo a todos los sectores de la población, en un esfuerzo abierto y multisectorial –gobierno, sector privado, comunidad técnica, academia y sociedad civil– que permita identificar las necesidades y opiniones de todos los sectores.

Principio 9. Recoger e implementar experiencias compartidas y buenas prácticas

Recoger e implementar experiencias y buenas prácticas de otras regiones en temas de seguridad digital –como las desarrolladas por la OCDE– y adaptarlas a las necesidades locales.

Principio 10. Adoptar estándares abierto de tecnología

Alentar a los gobiernos a adoptar políticas de seguridad digital públicas que incluyan su compromiso sobre el uso de productos que cumplan con estándares reconocidos de seguridad digital.

APORTES PARA UNA MEJOR COMPRENSIÓN DE LOS PRINCIPIOS

Principio 1. Abordar la seguridad digital desde los derechos humanos

Este principio atiende la necesidad de abordar la seguridad digital desde el enfoque de derechos humanos. Reconoce que el ciberespacio es importante para el ejercicio a la libertad expresión, la libre asociación, la privacidad, entro otros derechos. Además, recoge lo que el Consejo de Derechos Humanos de la Organización de las Naciones Unidas ha reiterado en 2012, 2014 y 2016: los derechos que las personas tienen fuera de internet también deben ser protegidos en línea.[7] Y en ese reconocimiento, los derechos humanos son el instrumento normativo que permite garantizar y llevar a cabo evaluaciones de los progresos en la seguridad de las personas a través de diferentes acciones estatales como lo son la formulación e implementación de políticas o estrategias nacionales de seguridad digital.

En ese proceso de formulación e implementación sirven de guía los instrumentos nacionales, regionales e internacionales de derechos humanos. Ahí se establecen las obligaciones de los Estados de proteger, por ejemplo, la libertad de expresión y el acceso a la información; el derecho de toda persona "a la vida, a la libertad y a la seguridad de la persona"; o la privacidad incluso de las comunicaciones digitales.[8] Esta normativa es la que debe ayudar a informar a los gobiernos a la hora de tomar decisiones sobre el ciberespacio que afecten o tengan impacto en los derechos de las personas.

7 *Véanse* las resoluciones no. 20/8 del 5 de julio de 2012, no. 26/13 del 26 de junio de 2014 y no. 32/13 de 27 de junio de 2016 del Consejo de Derechos Humanos de la ONU.
8 *Véanse*, por ejemplo, los artículo 3 y 19 de la *Declaración Universal de Derechos Humanos*; los artículo 4, 7 y 13 de la *Convención Americana de Derechos Humanos*; o la Resolución No. 68/167 de 21 de enero de 2014 de la Asamble General de la ONU sobre el derecho a la privacidad en la era digital.

El ciberespacio es, sin lugar a duda, un campo de tensión, en donde ocurren una multiplicidad de acciones por parte de gobiernos, empresas y/o individuos que atentan contra los derechos humanos: censura; control y manipulación de contenidos; retiro de contenidos en línea sin un debido proceso; filtraciones de datos personales; prácticas de los operadores y proveedores de servicios para limitar la calidad del acceso a fin de dar preferencia a ciertas aplicaciones y contenidos; aplicación radical de la legislación de propiedad intelectual, espionaje, cibercrimen, etc. Esto confirma la necesidad de abordar el tema de la seguridad digital desde un enfoque de derechos humanos.

No obstante, en la región de las Américas se observa una tendencia creciente a implementar prácticas violatorias de los derechos humanos en internet, en especial cuando de espionaje se trata. Por ejemplo, se sabe que varios países latinoamericanos compraron o intentaron comprar software de vigilancia que tiene la capacidad de registrar llamadas web, correo electrónico, mensajería instantánea, historial de navegación, etc.; además de que puede tomar control de los micrófonos, cámaras, archivos y fotos en los aparatos.[9] También se tienen pruebas, obtenidas mediante investigaciones científicas y tecnología forense, de que el Estado mexicano ha utilizado software malicioso de vigilancia contra funcionarios públicos, periodistas, opositores y activistas.[10] Y esto para nombrar algunos pocos ejemplos que dan cuenta del uso indebido e indiscriminado del espionaje estatal y de la adquisición de tecnología de vigilancia de las comunicaciones sin garantías de protección robustas y sin una adecuada implementación del debido proceso.

Este principio alienta a los países de la región a mejorar sus marcos legales sobre actividades de vigilancia. Los *Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones* (en adelante, Principios necesarios y proporcionales) y su guía de implementación pueden orientar la discusión a nivel nacional.[11] Los *Principios necesarios y proporcionales* son el resultado de una consulta

---

9 Pérez Acha, G. (2016, 20 de abril). *Hacking Team: El auge del software de vigilancia en América Latina* [blog post]. Disponible en https://www.derechosdigitales.org/9880/el-auge-del-software-de-vigilancia-en-america-latina/

10 *Véase* Artículo 19, Social TIC & R3D. (2017). *Gobierno Espía: Vigilancia sistemática a periodistas y defensores de derechos humanos en México.* Disponible en https://r3d.mx/gobiernoespia; Ahmed, A. & Perlroth, N. (2017, 19 de junio). Somos los nuevos enemigos del Estado': el espionaje a activistas y periodistas en México. *The New York Time*. Disponible en https://www.nytimes.com/es/2017/06/19/mexico-pegasus-nso-group-espionaje/

11 *Véase Necesarios & Proporcionados. Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones* de 10 de julio de 2014. Disponible en https://necessaryandproportionate.org/es/necesarios-proporcionados; y Access Now. (2015). *Universal Implementation Guide for the International Principles on the Application of Human Rights to Communications Surveillance.* Disponible en https://necessaryandproportionate.org/files/2016/04/01/implementation_guide_international_principles_2015.pdf.

global con grupos de la sociedad civil, la industria y personas expertas en derecho, política y tecnología de vigilancia de las comunicaciones, en donde se conceptualiza el derecho vigente en materia de derechos humanos frente a las tecnologías y técnicas modernas de vigilancia estatal. De este modo, "articulan los deberes y obligaciones de los Estados cuando participan en la vigilancia de las comunicaciones".[12]

Por otro lado, vale la pena presentar de manera sucinta 10 salvaguardas para las facultades estatales de intervención en sistemas informáticos que desarrolló la organización británica *Privacy International*, y que también pueden servir de guía para esta discusión:[13]

1. **Legalidad:** las facultades de vigilancia deben estar autorizadas por una ley que establezca límites claros y precisos, y que sea revisada periódicamente.

2. **Seguridad e integridad de los sistemas:** las autoridades gubernamentales deben realizar una evaluación sobre los riesgos y daños a la seguridad e integridad de las comunicaciones antes de llevar a cabo una medida de interferencia a las comunicaciones digitales. También deben incluir esta evaluación en cualquier solicitud de apoyo a dicha medida.

3. **Necesidad y proporcionalidad:** las autoridades gubernamentales deben establecer una serie de factores que permitan medir la probabilidad de ocurrencia de una amenaza contra un bien público protegido, información sobre el método, alcance y duración de la medida propuesta, y una evaluación de la seguridad. En cuanto a esta salvaguarda, *Privacy International* destaca que cuando se recurre al objetivo legítimo de la seguridad nacional como razón para intervenir comunicaciones digitales, los P*rincipios Siracusa de las Naciones Unidas sobre las Disposiciones de Limitación y Excepción en el Pacto Internacional de Derechos Civiles y Políticos* pueden orientar el alcance:

> La seguridad nacional puede ser invocada para justificar medidas que limiten ciertos derechos solo cuando se use para proteger la existencia de la nación, o su integridad territorial o independencia política contra la fuerza o la amenaza de fuerza [...] La seguridad nacional no puede invocarse como razón para imponer limitaciones a fin de prevenir amenazas meramente locales o relativamente aisladas a la ley y el orden[, o] como pretexto para imponer limitaciones vagas o arbitrarias (Traducción nuestra).[14]

12 Ibíd.
13 Privacy International. (2017, 15 de diciembre). *Government Hacking and Surveillance: 10 Necessary Safeguards.* Disponible en https://privacyinternational.org/node/957#9
14 *Principio Siracusa* citado en Ibíd.

4. **Autorización judicial:** una autoridad imparcial e independiente debe decidir si aprueba o no la medida y supervisar su aplicación. Esto también incluye la posibilidad de consultar a personas con conocimientos técnicos de las tecnologías a utilizarse y expertas en privacidad y derecho, que ayuden a informar cómo se pueden afectar los sistemas a intervenir y los derechos de la persona sujeta a la vigilancia.

5. **Integridad de la información:** como regla general, las autoridades gubernamentales no pueden añadir, alterar o borrar datos recolectados a través de la medida de intervención. Y si se usan los datos obtenidos, deben divulgar el método, alcance y duración de la medida, además del registro de las actividades empleadas.

6. **Notificación:** las autoridades gubernamentales deben notificar a las personas sujetas de vigilancia la fecha y duración de la medida, si los datos se obtuvieron o no de conformidad con la medida; y si los datos irrelevantes a la investigación se adquirieron con arreglo a la medida, como también la fecha de su destrucción.

7. **Destrucción y devolución de datos:** las autoridades gubernamentales deben establecer un procedimiento de destrucción de datos irrelevantes a la investigación, además de establecer un registro de este procedimiento. Esto también incluye el deber de los servicios de inteligencia de devolver los datos obtenidos a la persona destinataria y destruir cualquier copia de los datos al finalizar su uso.

8. **Supervisión y transparencia:** las autoridades gubernamentales deben someter sus facultades y actividades a un organismo de supervisión que sea independiente de los servicios de inteligencia y del poder ejecutivo, y que tengan acceso irrestricto a todos los aspectos de la labor de los servicios de inteligencia. Además, deben publicar, como mínimo, información relacionada con las solicitudes de autorización de las medidas de vigilancia de las comunicaciones digitales.

9. **Extraterritorialidad:** cuando se emplean medidas extraterritoriales de vigilancia, las autoridades gubernamentales deben cumplir sus obligaciones legales y abstenerse de utilizar estas medidas para eludir mecanismos legales (ej. tratados de asistencia legal mutua) de obtención de información fuera de su territorio.

10. **Remedios:** las personas sujetas a las medidas de intervención estatal ilegal deben tener acceso a un recurso efectivo, sin importar su lugar de residencia.

Además de lo anterior, creemos importante que se creen iniciativas regionales o globales para la evaluación de impacto de las políticas o estrategias nacionales de seguridad digital en los derechos humanos, que se explica en mayor detalle en el Principio 5. Igualmente, recomendamos desarrollar buenas prácticas y aprendizajes de lo que ha funcionado o no en la implementación de dichos planes. Esto incluye apoyar el trabajo de investigación en materia de seguridad que puede realizar, por ejemplo, un grupo de personas interesadas en la identificación y divulgación responsable de posibles vulnerabilidades de seguridad y privacidad. Esta práctica es explicada en mayor profundidad en el Principio 7.

Finalmente, le recomendamos al Comité Interamericano contra el Terrorismo (CICTE) de la OEA, que actualmente da asistencia a los países para fortalecer su capacidad técnica y de seguridad digital al nivel de políticas, le recomendamos que realice consultas y trabaje en conjunto con otras dependencias de la misma organización. Esto permitiría que sus recomendaciones estén alineadas con los estándares de libertad de expresión y privacidad elaborados por la Comisión y la Corte Interamericana de Derechos Humanos y la Relatoría Especial para la Libertad de Expresión (RELE) de la Comisión Interamericana de Derechos Humanos (CIDH).

Principio 2. Sustituir el concepto de ciberseguridad por seguridad digital

El concepto de seguridad en el ámbito cibernético o digital está en pleno desarrollo a nivel mundial y una definición específica ocultaría la discrepancia entre diferentes miradas, perspectivas e intereses. Esta disputa conceptual es la que ha permitido incorporar diversos temas a la discusión actual como, por ejemplo, los derechos humanos, la seguridad de las aplicaciones y servicios, la seguridad de las personas y de las infraestructuras a nivel nacional y de internet, etc. Todos estos temas permiten profundizar en el concepto en cuestión y trabajar sobre diferentes tipos y niveles de riesgos, enriqueciendo y fortaleciendo el abordaje

En general, la definición de seguridad digital–ciberseguridad, como más comúnmente se le llama– utilizada por los Estados es la elaborada por la UIT.[15] Sin embargo, cada Estado tiene intereses distintos ya sea sobre cómo se va a regular una actividad en internet, cuál debería ser su conceptualización y alcances, o qué actividades podrían constituir delitos. Por eso resulta complejo llegar a un acuerdo sobre una definición y se deben considerar

15 UIT. (2010). Resolution No. 181. *Definitions and terminology relating to building confidence and security in the use of information and communication technologies*. Disponible en https://www.itu.int/osg/csd/cybersecurity/WSIS/RESOLUTION_181.pdf.

múltiples factores.

Ya en 2013, la RELE-CIDH anotó la evolución que ha tenido este concepto:

> El concepto de ciberseguridad suele emplearse como un término amplio para referirse a diversos temas desde la seguridad de la infraestructura nacional y de las redes a través de las cuales se provee el servicio de Internet, hasta la seguridad o integridad de los usuarios [sic]. No obstante, desarrollos posteriores sugieren la necesidad de limitar el concepto exclusivamente al resguardo de los sistemas y datos informáticos [...] este enfoque acotado permite una mejor comprensión del problema así como una adecuada identificación de las soluciones necesarias para proteger las redes interdependientes y la infraestructura de la información.[16]

Como mencionamos en la introducción, la valoración más cercana al enfoque integrador, que relaciona la seguridad digital con el respeto a los derechos humanos, es la desarrollada en 2014 por el grupo de trabajo 1 de la *Freedom Online Coalition:*

> La ciberseguridad es la preservación – a través de políticas, tecnología y educación – de la disponibilidad, confidencialidad e integridad de la información y su infraestructura subyacente, a fin de mejorar la seguridad de las personas tanto *online* como *offline*.

Actualmente, las políticas o estrategias nacionales de seguridad digital tienen un "enfoque de daño". En su planteamiento de problema y desarrollo, suelen citar incidentes cibernéticos, crímenes, negligencias y ataques delincuenciales como fuente de los problemas centrales de la seguridad, a la vez que proponen mitigarlos con programas de educación. Sin embargo, el núcleo esencial de los planes debería ser la confidencialidad, integridad y disponibilidad de la información como la clave del componente técnico en la definición de ciberseguridad, tal como plantea la *Freedom Online Coalition*.[17]

La falta de terminología clara que permita establecer alcances y limitaciones de las acciones del Estado podría tener derivaciones e implicaciones desafortunadas. Algunas de ellas pueden ser la superposición –e incluso contradicción– de criterios de implementación de las políticas de seguridad entre las diferentes reparticiones del Estado y de los gobiernos; la adopción de medidas discrecionales por parte del funcionariado

16 CIDH. (2013, 31 de diciembre). *Libertad de expresión e Internet*. OEA/Ser.L/V/II CIDH/RELE/INF.11/13. Disponible en https://www.oas.org/es/cidh/expresion/docs/informes/2014_04_08_Internet_WEB.pdf.
17 La confidencialidad, la integridad y la disponibilidad son principios que guían la Certificación ISO 27001 sobre sistema de gestión de la seguridad de la información. Disponible en https://www.aenor.es/AENOR/certificacion/seguridad/seguridad_27001.asp.

sin ningún tipo de control o supervisión; el mantenimiento de prácticas opacas y la falta de transparencia, etc. En definitiva, se puede generar un escenario propicio para la vulneración de los derechos humanos.

Es necesaria una aproximación holística a las políticas de seguridad nacional donde el contexto se convierte en parte importante para su definición. La misma debe ser matizada y escalonada contemplando disposiciones, actores y tipos de riesgo. También debe incluir el enfoque de derechos humanos, en particular con consideración a la privacidad y a la libertad de expresión, así como un enfoque económico, siendo ambos centrales en la definición.[18]

Sustituir el concepto de *ciberseguridad* por *seguridad digital* sería una primera gran oportunidad para situar el discurso en aspectos relevantes del tema. En un sentido sustantivo, la seguridad es un concepto positivo, pues se refiere a la capacidad de una persona a acceder a un recurso fundamental y utilizarlo de acuerdo a sus necesidades y preferencias. Desde la óptica de los derechos humanos, la seguridad se centra en la capacidad de las personas de actuar libre y responsablemente. La política de seguridad en internet no debería limitarse a desempeñar un papel defensivo sino facilitador. Así, se potenciaría el bienestar de las personas como eje central. De esta forma, se aseguran soluciones con menos amenazas a los derechos humanos, garantías fundamentales de los sistemas democráticos.

A su vez, sería pertinente analizar la experiencia de Colombia, donde la Organización para la Cooperación y el Desarrollo Económicos (OCDE) sugirió la adopción del término "seguridad digital" en lugar de "ciberseguridad" en el Plan Nacional de Seguridad Digital, que en su fase de diagnóstico tuvo el apoyo de la OEA.[19] El proceso y el impacto que tendrá esta decisión merece la atención de los actores involucrados en el desarrollo y monitoreo de políticas de seguridad digital.

Principio 3. Favorecer prácticas de transparencia y rendición de cuentas

Será indispensable tomar medidas que puedan comprobar el alcance de las metas asumidas en las políticas públicas sobre seguridad digital. Para ello, es necesario avanzar en la articulación de políticas, transparencia y monitoreo de la gestión sobre este tema, lo que implica verificar si se ha cumplido con lo programado y luego evaluar

18 Internet Society. (2015, 12 de april). *Collaborative Security: An approach to tackling Internet Security Issues.* Disponible en https://www.internetsociety.org/collaborativesecurity
19 Ministerio TIC. (2016, 15 de abril). *Colombia cuenta con una Política Nacional de Seguridad Digital*. Disponible en http://www.mintic.gov.co/portal/604/w3-article-15033.html

los resultados obtenidos. Esta mirada al pasado permite observar cuál ha sido el punto de partida –es decir, la línea de base– y cuáles han sido los avances logrados. De esa forma, también se fomenta la confianza en el ciberespacio y la economía digital.

La articulación o coordinación de políticas públicas es un factor importante para el diálogo entre unidades gubernamentales que cogestionan la solución de problemas transectoriales en temas de seguridad digital. La rendición de cuentas es la herramienta más apropiada para visibilizar las acciones que se toman para estos temas, pues ayuda a prevenir y controlar cualquier abuso, además de que incrementa la seguridad digital de todas las personas.

Al respecto, Carlos Santiso del Banco Interamericano de Desarrollo (BID) señala:

> La transparencia construye la ciudadanía. La región de América Latina y el Caribe es compromiso con un gobierno abierto y transparente, no sólo [sic] porque es una herramienta para prevenir y controlar corrupción, sino también porque fortalece la democracia y mejora la efectividad del Estado, especialmente en la prestación de servicios públicos. Transforma la cultura burocrática introduciendo contrapesos discrecionales. Mejora la eficiencia y disminuye las posibilidades de fraude y corrupción en gestión pública, reduciendo el número de pasos y transacciones y maximiza el uso de las nuevas tecnologías. La transparencia permite rendición de cuentas.[20]

Por otro lado, en la *Declaración de Seúl sobre el futuro de la economía de internet*, la OCDE aboga por los principios de transparencia y rendición de cuentas, reconociendo que contribuyen a una libre circulación de la información, a la libertad de expresión y a la protección de las libertades individuales.[21]

Asimismo, para la OCDE, el principio de transparencia es uno de los

> pilares centrales de una reglamentación efectiva, el mantenimiento de la confianza en el entorno jurídico, fortaleciendo regulaciones seguras y accesibles, menos influenciadas por intereses especiales y, por tanto, más competitiva y abierta al comercio e inversión (Traducción nuestra).[22]

---

20 Santiso, C. (2017, 26 de febrero). Cómo los datos ayudan a destapar la corrupción [blog post]. *Gobernarte: ideas innovadoras para mejorar gobiernos.* Disponible en https://blogs.iadb.org/gobernarte/2017/02/28/los-datos-ayudan-destapar-la-corrupcion/

21 OCDE. (2013). *The Internet Economy on the Rise: Progress since the Seoul Declaration.* Disponible en http://www.oecd.org/futureinternet/.

22 Global Partnership for Effective Development Co-operation. (2016, 3 de noviembre). The Transparency Chapter of the GPEDC Monitoring report. *Making Development Co-operation More Effective: 2016 Progress Report*. Disponible en https://www.oecd.org/dac/effectiveness/making-development-co-operation-more-effective-9789264266261-en.htm.

Por todo esto, los indicadores propuestos en las políticas o estrategias de seguridad digital deberán ser medibles y verificables. El cumplimiento de las metas trazadas no debe terminar en una mera declaración de buenas intenciones, sino que sus resultados deben promover la confianza en el ciberespacio. La metodología utilizada en gobierno abierto puede ayudar a mejorar la aplicación de estos planes.

Además, se debe dar lugar al aporte de la ciudadanía y la sociedad civil, que desarrollamos con más detalles en el Principio 8, en procesos de formulación de políticas públicas más saludables para una gestión estatal en seguridad digital. Su papel activo corresponde a la formulación conjunta de políticas, coproductor de bienes y servicios públicos, y como fiscalizador de los resultados de la acción gubernamental.[23]

Por otro lado, los espacios de gobierno abierto deben incluir mesas de diálogo sobre seguridad digital.[24] En sus agendas de discusión en temas de tecnología, deberían tratarse asuntos como la protección de los derechos humanos a través del uso del cifrado como una estrategia efectiva contra la vigilancia masiva, entre otros.

Gran parte de la economía de internet depende de recolectar datos complejos sobre potenciales clientes para venderles productos y servicios, una práctica conocida como "capitalismo de la vigilancia".[25] Por lo tanto, es clave que los planes de gobierno abierto no solo aboguen por la apertura de datos, sino también por la protección de los mismos para evitar riesgos y abusos por parte del sistema actual. Así, se contribuye a que se implementen estándares mínimos de protección de los derechos humanos en el desarrollo de economía basada en datos.[26]

En este sentido, el informe del grupo de trabajo de *big data* y datos abiertos, establecido por el Relator Especial de la ONU sobre el derecho a la privacidad, destaca que

> Cualquier iniciativa de gobierno abierto que implique información personal, ya sea anonimizada o no, requiere un análisis riguroso, público y científico de las

23 Oszlak, O. (2013). *Gobierno abierto: hacia un nuevo paradigma de gestión pública.* Disponible en https://www.oas.org/es/sap/dgpe/pub/coleccion5RG.pdf.
24 *Véase* el sitio web del *Open Government Partnership* en https://www.opengovpartnership.org.
25 Zuboff, S. (2015, 17 de abril). Big Other: Surveillance Capitalism and the Prospects of an Information Civilization. *Journal of Information Technology*, 30, pp. 75–89. DOI: https://doi.org/10.1057/jit.2015.5.
26 Las corporaciones y los gobiernos no necesariamente tienen que ser forzados a proporcionar protecciones de privacidad. Véase, por ejemplo, enfoques éticos adoptados por las empresas en Information Commissioner's Office. (2017). *Big data, artificial intelligence, machine learning and data protection.* Disponible en https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf.

> protecciones de la privacidad de los datos, incluida una evaluación del impacto sobre la privacidad (Traducción nuestra).[27]

Todas estas propuestas ayudan a promover una mayor transparencia inter e intra gubernamental, además de fomentar la confianza en internet y garantizar el éxito continuado de la misma como motor de innovación socioeconómica. En este ámbito de cooperación, se deberán garantizar la transparencia, la rendición de cuentas y la articulación de políticas en lo que respecta a las prácticas en el entorno digital, así como al cumplimiento de los compromisos asumidos por los Estados en los planes de acción de gobierno abierto. Las estadísticas sobre las vulnerabilidades informáticas deberán ser accesibles y reutilizables por todas las personas, pues serán clave para abordar la política de seguridad digital de forma conjunta, según explicamos en mayor detalle en el Principio 6.

Principio 4. Promover y respetar el uso del cifrado

La seguridad y privacidad son caras de una misma moneda. Se refuerzan mutuamente y generan entornos saludables para la confianza de las personas en la red, contribuyen al florecimiento de una variedad de servicios en internet. La adopción de buenas prácticas en seguridad y privacidad deberían incluirse en las políticas o estrategias nacionales de seguridad digital, así como establecer salvaguardas nacionales para la promoción de herramientas de cifrado y otros sistemas de protección para las personas.

En este sentido, vale la pena entender que el cifrado, proceso por el que se codifican los datos utilizando algoritmos matemáticos, ayuda a proteger la información de una comunicación o en cualquier dispositivo en la que se encuentre. En el caso de las comunicaciones en internet, se recomienda la criptografía de clave pública.[28] Las

27 Véase *Surveillance, big data and open data top UN expert's privacy agenda*. (2017, 20 de octubre). Disponible en http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=22271&LangID=E

28 La criptografía se ocupa de las técnicas de cifrado o codificado destinadas a alterar las representaciones lingüísticas de ciertos mensajes con el fin de hacerlos ininteligibles a receptores no autorizados, con el objetivo de conseguir la confidencialidad de los mensajes. La criptografía asimétrica, también llamada criptografía de clave pública, utiliza un par de claves para el envío de mensajes. Las dos claves pertenecen a la misma persona que ha enviado el mensaje. Una clave es pública y se puede entregar a cualquier persona, la otra clave es privada y quien sea propietaria debe guardarla de modo que nadie tenga acceso a ella. Además, los métodos criptográficos garantizan que esa pareja de claves solo se puede generar una vez, de modo que se puede asumir que no es posible que dos personas hayan obtenido casualmente la misma pareja de claves. Criptografía asimétrica. (s.f.). Wikipedia. Disponible en https://es.wikipedia.org/wiki/Criptografía_asimétrica

herramientas criptográficas de código abierto[29] son una condición necesaria para garantizar las comunicaciones seguras en la actualidad, ya que habilitan la auditoría y reducen potencialmente la introducción de funcionalidad maliciosa.[30]

Por otro lado, el cifrado se utiliza para construir mayor seguridad para las transacciones financieras, el comercio electrónico, las comunicaciones militares, entre otros usos, y no debería estar limitado solamente a ciertos grupos, sino que debe abarcar a todos los sectores sociales.[31] El cifrado aporta confianza en las comunicaciones porque permite asegurar la identidad de los dispositivos implicados, a la vez que garantiza la integridad de los datos, evitando su manipulación. Una navegación o comunicación que no esté cifrada no está simplemente "poco cifrada": en realidad, se encuentra abierta a todo tipo de posibles abusos.[32] Además, es simple y fácil implementar el cifrado, al punto de que hoy en día vivimos cifrando información sin darnos cuenta (ej. cifrado de extremo a extremo de WhatsApp).

En este sentido, es necesario que las recomendaciones de seguridad digital de organismos internacionales (ej. la OEA), así como las políticas o estrategias nacionales que formulen los Estados, incluyan el uso del cifrado como formas de defender la privacidad y libertad de expresión de las personas. Como se ha mencionado antes, las estrategias de seguridad digital deben ser diseñadas e implementadas de manera consistente con el derecho internacional de los derechos humanos. Por ejemplo, el derecho a la privacidad debe ser un componente central en el desarrollo de una política o estrategia de seguridad. Estos principios deben ser explicitados en el plan, tanto en su desarrollo como en sus anexos.

Como se examinó en el Principio 1, los antecedentes regionales de adquisición y uso de tecnología de vigilancia, y de espionaje estatal evidencian la necesidad de políticas o estrategias de seguridad digital que consideren acciones concretas a través de la

29 El código abierto es un modelo de desarrollo de software basado en la colaboración abierta. Se enfoca más en los beneficios prácticos (acceso al código fuente) que en cuestiones éticas o de libertad que tanto se destacan en el software libre. Levine, S.S. & Prietula, M. (2014). Open Collaboration for Innovation: Principles and Performance. *Social Science Research Network,* 25(5). Disponible en http://dx.doi.org/10.2139/ssrn.1096442.

30 Schneier, B. (1999, 15 de septiembre). Open Source and Security. *Crypto-Gram*. Disponible en https://www.schneier.com/crypto-gram/archives/1999/0915.html#OpenSourceandSecurity

31 Privacy International. (2015). *Securing Safe Space Online: Encryption, online anonymity, and human rights.* Disponible en https://www.privacyinternational.org/report/1118/securing-safe-spaces-online-encryption-online-anonymity-and-human-rights

32 Kambo, H. (2015, 4 de septiembre). *The pincer movement against encryption* [blog post]. Disponible en https://www.privacyinternational.org/node/641.

cooperación internacional y alianzas con otros sectores.[33] Además, reiteramos que deben estar en línea con los estándares de protección de los derechos fundamentales.

Para prevenir estos riesgos, se deben desarrollar políticas de cifrado de las comunicaciones y navegación en internet que contemplen indicadores esenciales para el ejercicio pleno de las libertades individuales. Estas deben incluir la creación de indicadores de transparencia en el desarrollo de software, pues es la única forma de garantizar un cifrado confiable y auditable de forma colectiva. En este sentido, se ha demostrado que la "seguridad por transparencia" es más eficaz en la solución de fallos y, por lo tanto, se vuelve un elemento clave para la seguridad informática.[34]

A su vez, esto dificultaría el robo de información y la inclusión de puertas traseras, que hoy ponen en peligro a las personas que legítimamente usan software de comunicación cifrada, sin que disminuya la probabilidad de uso de personas con intenciones criminales.[35] Estos actores maliciosos probablemente encontrarán otros medios de comunicación, mientras que la mayoría de las personas no tendrán disponibles las mismas herramientas. De esta forma, se genera una asimetría y efectos perjudiciales para la mayoría de la población, ya que los gobiernos y actores maliciosos pueden explotar y abusar de dichas puertas traseras.

La confianza de las personas es fundamental para el crecimiento y la evolución de internet. La misma genera valoraciones positivas en el uso de aplicaciones y servicios seguros que sean respetuosos de la privacidad. Por lo tanto, es indispensable el fomento de mecanismos confiables para la autenticación, confidencialidad e integridad de los datos como componentes vitales para la construcción de productos y servicios de confianza.

David Kaye, Relator especial de la ONU para la libertad de expresión, en su informe sobre la importancia del cifrado y el anonimato para la libertad de expresión, manifestó que "el cifrado y el anonimato proporcionan la privacidad y la seguridad necesarias para el ejercicio de la libertad de opinión y de expresión en la era digital" (Traducción nuestra).[36]

33 *Véase* la nota 10.
34 Challet, D., & Du, Y. L. (2005, 5 de septiembre). Microscopic Model of Software Bug Dynamics: Closed Source Versus Open Source. *International Journal of Reliability, Quality and Safety Engineering.* Disponible en http://arxiv.org/pdf/condmat/0306511.pdf
35 Una puerta trasera es una técnica informática que implica la introducción de una secuencia de programación dentro del código fuente que permite evitar los sistemas de seguridad. Tal como su nombre lo indica, es una forma de ingresar a un sistema "por la parte de atrás".
36 Kaye, D. (2015, 22 de mayo). *Report on encryption, anonymity, and the human rights framework.* A/HRC/29/32. Disponible en http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/CallForSubmission.aspx

Siguiendo esa premisa, el Relator recomienda, entre otras cosas, que "las legislaciones nacionales [reconozcan] que los individuos son libres de proteger la privacidad de sus comunicaciones digitales mediante el uso de tecnologías de cifrado y herramientas que permiten el anonimato en línea" (Traducción nuestra).[37]

También destaca que se debe promover el acceso a estas herramientas y tecnologías, más allá de que los debates sobre cifrado y anonimato hayan sido polarizados por su uso potencialmente criminal. Por lo tanto, se propone un cambio en el debate para destacar la protección que estas tecnologías ofrecen a los individuos, especialmente a los grupos que viven en situación de riesgo: periodistas, personas que defienden los derechos humanos, activistas de derechos sexuales y reproductivos, activistas que luchan por el reconocimiento político y social de la diversidad sexual y de género, etc.

Principio 5. Usar análisis de privacidad por diseño y de impacto en derechos humanos

El concepto de privacidad por diseño[38] implica que las medidas de privacidad sean operativas a lo largo de todo el ciclo de vida de las tecnologías, desde la fase inicial de diseño hasta su implementación, uso y eliminación definitiva.[39] Si bien la privacidad por diseño nace como un concepto ligado al desarrollo de las tecnologías, esto no implica que quede solo relegado a dicho ámbito. Por el contrario, su filosofía puede ser implementada en diversos campos como en la formulación de leyes y regulaciones, o en el desarrollo de políticas públicas.

37 Ibíd, párr. 8.

38 El concepto de "privacidad por diseño" comienza a escucharse por primera vez en el año 1995, partiendo de la base del concepto "*privacy-enhancing technologies*" o tecnologías que mejoran la privacidad, que aparece en un informe conjunto publicado por el Comisionado de Información de Ontario, la Autoridad Neerlandesa de Protección de Datos y la Organización de los Países Bajos para la Investigación Científica Aplicada. Para conocer más al respecto, véase Hes, R. & Borking, J. (eds.; 2000). Privacy-Enhancing Technologies: The Path to Anonymity. Revised edition. *Achtergrondstudies en Verkenningen,* 11.
Disponible en https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/av/av11.pdf; Botero, C. (2015, 17 de noviembre). *¿Qué es la privacidad por diseño y por qué debería importarle?* [blog post]. Disponible en https://karisma.org.co/que-es-la-privacidad-por-diseno-y-por-que-deberia-importarle/.

39 van Rest J., et al. (2014) Designing Privacy-by-Design. En Preneel B. & Ikonomou D. (eds.; 2012). Privacy Technologies and Policy. *Lecture Notes in Computer Science*, 8319. Disponible en https://link.springer.com/chapter/10.1007/978-3-642-54069-1_4.

La implementación de la privacidad por diseño está centrada en 7 principios guía:[40]

1. Las medidas deben ser proactivas, no reactivas. Es decir, se evita que ocurran –anticipando y previniendo– incidentes o eventos que pueden interferir con la privacidad antes de que sucedan.

2. La privacidad debe estar implementada de forma predeterminada. No debe requerirse ninguna acción especial por parte de las personas para proteger su privacidad. Esto brindará la máxima protección posible para su privacidad.

3. La privacidad debe estar integrada en el diseño y arquitectura de los sistemas de tecnologías de la información y en las prácticas de las empresas en forma holística. Es un componente de las funcionalidades básicas brindadas que debe integrarse al sistema sin afectar su operación.

4. La funcionalidad siempre debe ser total. La privacidad por diseño busca acomodar todos los intereses y objetivos legítimos bajo un juego de suma positiva, es decir, todas las partes ganan.

5. La seguridad debe ser de extremo a extremo. La privacidad debe ser protegida a lo largo de todo el ciclo de vida de la tecnología o la información en cuestión, bajo estándares que aseguren la confidencialidad, integridad y disponibilidad de la información, y protocolos de cifrado que cuenten con la aprobación consensuada de las comunidades técnicas.

6. La privacidad por diseño debe ir de la mano de políticas de transparencia y visibilidad como forma de garantizar una adecuada rendición de cuentas y ganar la confianza de las personas.

7. El enfoque debe estar puesto en las personas. La privacidad por diseño requiere que el desarrollo de las tecnologías, prácticas, políticas, leyes o regulaciones se centren en las necesidades e intereses de las personas, quienes deben poder contar con la información suficiente para tomar decisiones adecuadas vinculadas a su privacidad.

40 Cavoukian, A. (2011). *Privacy by Design, the 7 Foundational Principles. Implementation and Mapping of Fair Information Practices.* Ontario, Canada: Information & Privacy Commissioner. Disponible en https://iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf.

A modo de ejemplo, podemos mencionar el caso de la Dirección Nacional de Protección de Datos Personales en Argentina, que en 2015 tomó el concepto y los principios de la privacidad por diseño para incluirlos en su *Guía de buenas prácticas en privacidad para el desarrollo de aplicaciones*.[41] También es relevante el *Reglamento General de Protección de Datos,* aprobado por el Parlamento Europeo en 2016, que adopta en su artículo 25 una variante de la privacidad por diseño sobre la protección de datos desde el diseño y por defecto.[42]

También vale la pena mencionar el informe de 2014 sobre privacidad y protección de datos personales por diseño elaborado por la Agencia de la Unión Europea para la Seguridad de las Redes y la Información (ENISA, por sus siglas en inglés).[43] El informe brinda un inventario sobre diversos enfoques, estrategias y técnicas de construcción de la privacidad por diseño, con el fin de facilitar las herramientas para poder implementarla efectivamente. En 2015, ENISA publicó un nuevo informe llevando el análisis de la privacidad por diseño al *big data*.[44] Entre las recomendaciones, la ENISA llama al poder legislativo a apoyar y promover el desarrollo de mecanismos que incentiven servicios que sean amigables con la privacidad, además de promover la privacidad y la protección de datos en las normativas. Por otra parte, establece que los organismos desarrolladores de estándares deben incluir consideraciones a la privacidad en sus procesos de estandarización. Las autoridades de protección de datos también deben jugar un papel importante proporcionando orientación independiente, y evaluando módulos y herramientas para la ingeniería de privacidad.

Con el fin de brindar lineamientos claros y precisos que respondan a cómo implementar la privacidad por diseño a partir de una metodología concreta, Nokia, la empresa finlandesa de telecomunicaciones, publicó el documento *Privacy Engineering & Assurance*, en el que detalla su estrategia para poner en funcionamiento una metodología que permita tender un puente entre el enfoque legal y el tecnológico, logrando la formación de profesionales especializados como ingenieros de privacidad.[45]

---

41 Ministerio de Justicia & Dirección Nacional de Protección de Datos Personales (2015, 10 de abril). *Guía de Buenas Prácticas en Privacidad para el Desarrollo de Aplicaciones.* Disposición N° 18/2015. Disponible en http://www.jus.gob.ar/media/2854264/disp_2015_18.pdf

42 Parlamento Europeo. (2016, 27 de abril). Reglamento general de protección de datos. Reglamento (UE) 2016/679. Disponible en http://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32016R0679&from=ES

43 Danezis, G. et al. (2014). *Privacy and Data Protection by Design*. Europe: ENISA. Disponible en https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design.

44 D'Acquisto G. (2015). *Privacy by design in big data.* ENISA. Disponible en https://www.enisa.europa.eu/publications/big-data-protection.

45 Nokia (2014). *Privacy Engineering & Assurance: The Emerging Engineering Discipline for implementing Privacy by Design*. Disponible en https://iapp.org/media/pdf/resource_center/Privacy_Engineering+assurance-Nokia_9-14.pdf

La metodología propuesta por Nokia se sustenta en una base de conocimiento sobre privacidad. Esto incluye principios; amenazas y sus vulnerabilidades de ingeniería subyacentes; riesgos; requisitos y pautas de protección; y patrones de diseño para implementar controles de protección de la privacidad. Esta disciplina cuenta con dos componentes. El primero es la "ingeniería de privacidad", que consiste en una etapa de planificación en donde se evalúan las amenazas y su mitigación, así como también la identificación de los requerimientos de privacidad. Luego, en las etapas de diseño, implementación y prueba, se diseñan y ejecutan los controles de protección de la privacidad en productos y servicios.

En segundo lugar, encontramos la "garantía de privacidad", en donde se verifica la conformidad de los productos y servicios con controles de protección a la privacidad y el cumplimiento normativo. A su vez, se contrastan cada uno de los puntos con la evidencia existente que permita dar cuenta del cumplimiento de cada etapa del proceso.

Ahora bien, cuando hablamos de los Estados y las evaluaciones de impacto en derechos humanos entra en acción el deber que tienen de proteger a su población. Esta responsabilidad conlleva obligaciones negativas y positivas. La primera de ellas implica no incurrir en acción alguna que pueda poner en peligro o directamente viole el ejercicio y goce de derechos humanos y libertades individuales. La segunda supone tomar medidas que ayuden a promover, garantizar e incentivar el libre y pleno ejercicio de dichos derechos y libertades.

Los *Principios Rectores sobre las empresas y los derechos humanos (en adelante, Principios Rectores)* de la ONU son un buena guía para explorar formas de implementación de evaluaciones de impacto en derechos humanos. En ellos se aclaran los deberes y responsabilidades de los Estados y las empresas con relación a la protección y respeto de los derechos humanos en el contexto de actividades empresariales.[46] Con el fin de identificar, prevenir, mitigar y responder a los impactos negativos sobre los derechos humanos de las actividades empresariales, los *Principios Rectores* establecen que las empresas deben proceder con la debida diligencia. En ese sentido, deben (1) evaluar el impacto actual y potencial en los derechos humanos; (2) actuar sobre los descubrimientos; (3) realizar el seguimiento del rendimiento de dicha actuación; y (4) comunicar cómo se está trabajando en el impacto actual y potencial identificado inicialmente.

46 ONU. (2014). Preguntas frecuentes acerca de los principios rectores sobre las empresas y los derechos humanos. HR/PUB/14/3, p. 6. Disponible en http://www.ohchr.org/Documents/Publications/FAQ_PrinciplesBussinessHR_SP.pdf.

Para simplificar este proceso, tanto las empresas como los Estados deberían llevar a cabo evaluaciones de impacto en derechos humanos, evaluar los riesgos para las personas titulares de derechos –no solo para la empresa o el Estado–, y la capacidad de quienes tienen deberes. Los instrumentos en los que se debe basar dicha evaluación, como se mencionó en el Principio 1, son los comprendidos en la *Carta Internacional de Derechos Humanos,* que consiste en la *Declaración Universal de los Derechos Humanos* y el *Pacto Internacional de Derechos Civiles y Políticos,* el *Pacto Internacional de Derechos Económicos, Sociales y Culturales,* y sus protocolos facultativos.[47]

Principio 6. Desarrollar CSIRT independientes de las fuerzas del orden público

Ante un eventual incidente de seguridad informática, las personas que utilizan la tecnología cotidianamente –e incluso quienes no son usuarias– son las que ven expuestos sus datos. Paradójicamente, son ellas las más desprotegidas, pues encuentran grandes dificultades para resolver la situación y tomar acciones que eviten una nueva ocurrencia. Algunas empresas ocultan sus incidentes de seguridad, a pesar de que, muchas veces, implique filtración de información. En estos escenarios, las personas son las damnificadas. Este tipo de comportamientos suele deberse al miedo a perder reputación, a que su imagen como empresa quede dañada y/o a que, ulteriormente, tengan que responder legalmente por su negligencia.

A medida que se incorporan más personas al ciberespacio y crece el volumen de información de todo tipo –incluyendo información personal, sensible, económica, etc.- internet se vuelve un blanco de interés para actores maliciosos que buscan explotar las vulnerabilidades de la infraestructura de la red. Según señalan investigaciones en seguridad informática, hay una tendencia creciente en la industrialización del cibercrimen, que incluye cadenas de profesionales especializados en desarrollo de software, ejecución de las operaciones y hasta en lavado de dinero, que se manejan como verdaderos negocios en un campo altamente competitivo.[48]

Podemos afirmar entonces que tanto en el sector privado como en el público existen actores y situaciones que ponen en riesgo la seguridad de las personas y de la sociedad civil, convirtiéndose en una compleja problemática multidimensional. Frente a este escenario,

47 Ruggie, J. (2007, 5 de febrero). *Evaluaciones de impacto sobre los derechos humanos: resolución de cuestiones metodológicas esenciales*. A/HRC/4/74. Disponible en http://www.ohchr.org/EN/Issues/TransnationalCorporations/Pages/Reports.aspx

48 Goodman, M. (2015), *Future Crimes: Everything is Connected, Everyone is Vulnerable and What We Can Do About It*. New York, USA: Random House.

queda en evidencia la necesidad de contar con un organismo que pueda responder ante las problemáticas, urgencias e inquietudes de la sociedad civil, reconociendo que la misma se encuentra en una posición de desventaja con respecto a posibles abusos de terceros. Es allí donde el rol de los equipos de respuesta a incidentes de seguridad informática (CSIRT, por sus siglas en inglés) se vuelve crucial para prevenir, gestionar y responder a incidentes de seguridad de la información.

En América Latina, los CSIRT o CERT surgen principalmente en el ámbito gubernamental, respondiendo a necesidades latentes de los Estados de proteger sus datos, sistemas e infraestructuras críticas. Tal es el caso de Argentina, Brasil, Bolivia, Chile, Colombia, Costa Rica, Ecuador, Guatemala, México, Paraguay, Perú, Uruguay y Venezuela.[49]

Dado todo este contexto y ante el posible crecimiento exponencial de los incidentes de seguridad informática, se vuelve urgente y necesario promover equipos de respuesta que sean independientes e imparciales, y que trabajen por la protección de las infraestructuras, la información y la seguridad de las personas que utilizan las tecnologías. Esto permitirá una respuesta más efectiva que garantice el pleno desarrollo de la sociedad civil en el ámbito digital.

Actualmente, es cada vez más común ver a diversos CSIRT alrededor del mundo adoptar una actitud más proactiva. Hoy no solo actúan ante una emergencia, sino que trabajan para brindar servicios de prevención y detección de incidentes. Incluso elaboran documentos que sugieren la implementación de buenas prácticas de seguridad informática, y comunican y difunden vulnerabilidades vinculadas con la seguridad de la información. Este tipo de acciones está permitiendo identificar patrones de ataque o sistematizar problemas comunes con el fin de prevenirlos o mitigarlos.

A comienzos de 2016, la OEA publicó una guía de buenas prácticas para establecer un CSIRT nacional. El documento analiza el proceso de creación y puesta en marcha de un CSIRT, con diversas consideraciones respecto a su misión, visión, alcance, servicios, aspectos legales, institucionales y organizacionales, recursos humanos, infraestructura, así como también las diferentes políticas y procedimientos para asegurar la fluidez en las operaciones.[50] Este documento también puede servirle a los Estados al momento de considerar la puesta en marcha de CSIRT sectoriales independientes e imparciales.

49 BID & OEA. (2016). *Informe Ciberseguridad 2016. ¿Estamos preparados en América Latina y el Caribe?*. Disponible en http://www.iadb.org/es/noticias/comunicados-de-prensa/2016-03-14/informe-sobre-ciberseguridad-en-america-latina,11420.html.

50 OEA (2016). Buenas prácticas para establecer un CSIRT nacional. Programa de Seguridad Cibernética. Disponible en: https://www.sites.oas.org/cyber/Documents/2016%20-%20Buenas%20Practicas%20CSIRT.pdf

Para esclarecer este punto, podríamos hacer un paralelismo del ámbito analógico con el digital, y tomar como ejemplo el caso de la Cruz Roja y su respuesta humanitaria ante escenarios bélicos o desastres naturales.[51] Esta organización fundada en 1859 mantiene una esencia de neutralidad, lo que implica no involucrarse o tomar posición con ningún bando en las crisis ante las que proporciona su asistencia o protección, que es brindada de forma imparcial, sin discriminación o preocupación por la identidad de las víctimas o su actividad previa. Además, mantiene una independencia que le permite no estar atada a la agenda de ningún actor gubernamental en particular.[52]

Contar con CSIRT independientes e imparciales representaría un gran avance en la construcción de confianza en el ciberespacio. Comenzando por la reorientación del análisis de la seguridad digital hacia la mejora de la seguridad de las personas, y evitando los juegos de suma-cero, así como los argumentos de securitización.

Por último, cabe recordar que la función esencial de los CSIRT incluye la coordinación de respuesta y el intercambio de información y difusión en lo referente a incidentes informáticos. Cuando hablamos del desarrollo de políticas o estrategias nacionales de seguridad digital, la facultad de contar con las herramientas y recursos para producir información y datos se vuelve imprescindible. Tener certezas sobre las cuales construir la estrategia y el plan de acción de seguridad digital, conociendo las problemáticas que enfrentan los diversos sectores de la sociedad, debería ser un requisito *sine qua non,* pues es la única forma de comprender los riesgos y necesidades de las personas usuarias de las tecnologías.

Principio 7. Apoyar buenas prácticas de seguridad digital en los sistemas informáticos

En el campo de la seguridad informática, una de las prácticas más comunes es la investigación de vulnerabilidades, es decir, la búsqueda de debilidades del sistema que le permiten a un agente externo obtener acceso, generalmente con fines espúreos, impactando negativamente en la integridad, confidencialidad o disponibilidad del sistema.[53] Estas debilidades son el resultado de fallos en el diseño del sistema o a veces simplemente limitaciones tecnológicas.

51 *Véase* Cruz Roja Internacional. (s.f.). El movimiento internacional de la Cruz Roja y de la Media Luna Roja [blog post]. Disponible en http://www.ifrc.org/es/nuestra-vision-nuestra-mision/movimiento/.
52 Hollis, D. & Maurer, T. (2015, 18 de febrero). A Red Cross for Cyberspace. *Time.* Disponible en http://time.com/3713226/red-cross-cyberspace/.
53 *Véase* el sitio web de *Common Vulnerabilities and Exposures* en https://cve.mitre.org/about/terminology.html.

Bruce Schneier, experto internacional en seguridad informática, establece que el escrutinio público es necesario para mejorar la seguridad de los sistemas. Alienta la búsqueda y revelación de vulnerabilidades, en contraposición a la "seguridad por oscuridad", ya que el secretismo impide la posibilidad de evaluar el riesgo, a la vez que excluye el debate público e inhibe el potencial de aprendizaje sobre seguridad informática.[54]

Actualmente, se pueden encontrar empresas que mantienen programas de recompensa por errores o *bug bounty,* con los que se busca reconocer y recompensar a quienes reporten vulnerabilidades de los sistemas informáticos.[55] Esto les permite a las empresas incentivar a estudiantes, hackers y personas expertas vulnerabilidades y reducir la probabilidad de incidentes a causa del uso generalizado de debilidades desconocidas (*zero-days*).

Esta práctica puede ser adoptada por los Estados con el fin de alentar y apoyar el trabajo de investigación en materia de seguridad. De esta forma y con apoyo de personas interesadas actuando de buena fe, se puede identificar y compartir responsablemente las vulnerabilidades de seguridad y privacidad detectadas en las diversas implementaciones tecnológicas que los mismos Estados llevan a cabo en su relación con la ciudadanía.

Para poner en marcha esta práctica, es necesario que los Estados creen canales de comunicación y protocolos de actuación frente a la identificación de vulnerabilidades de grupos o individuos que realizan auditorías independientes en sistemas de información del Estado. A comienzos de 2016, el Gobierno de los Estados Unidos lanzó su primer *bug bounty, Hack the Pentagon*, con el objetivo de identificar vulnerabilidades en su red, analizar la seguridad de sus sitios web públicos y la robustez de sus sistemas ante potenciales intrusiones.[56] Esta iniciativa puede servir de inspiración para los Estados latinoamericanos adaptándola a sus propios contextos, dejando atrás otras prácticas que terminan perjudicando al ecosistema de la seguridad informática, en ocasiones acarreando graves consecuencias para las personas que trabajaron en reportar las vulnerabilidades.[57]

54 Schneier, B. (2007). *Full Disclosure of Security Vulnerabilities a 'Damned Good Idea'* [blog post]. Disponible en https://www.schneier.com/essays/archives/2007/01/schneier_full_disclo.html.

55 A modo de ejemplo, podemos mencionar empresas como Apple, Microsoft, Mozilla (https://www.mozilla.org/en-US/security/bug-bounty/), Google (https://www.google.com/about/app-security/programs-home/) y Facebook (https://www.facebook.com/whitehat).

56 Carman, A. (2016, 2 de marzo). The US government just launched its first bug bounty program. *The Verge*. Disponible en https://www.theverge.com/2016/3/2/11146420/hack-the-pentagon-department-of-defense-bug-bounty.

57 En tal sentido, destacamos con preocupación dos casos. El primero de ellos ocurrió en Colombia, cuando ante el reporte de vulnerabilidades de la plataforma de censo digital, el Departamento Administrativo Nacional de Estadística (DANE) optó por desacreditar públicamente a la persona que había reportado los problemas de seguridad. *Véase Botero,* C. (2018, 18 de enero). Lección 1 del e-censo: no matar a la mensajera. El Espectador. Disponible en https://www.elespectador.com/opinion/leccion-1-del-e-censo-no-matar-la-mensajera-columna-734171 El segundo caso ocurrió en Argentina, cuando un programador que reportó vulnerabili-

De otra parte, es fundamental que los Estados promuevan e implemente la práctica de utilizar programas informáticos actualizados con las últimas correcciones de seguridad, de modo que no se reduzcan los riesgos digitales de las personas.. Esto es aún más importante cuando se considera que las actividades en línea pueden tener consecuencias directas en la vida diaria de las personas como, por ejemplo, la administración en línea de las finanzas personales (*home banking*), el pago de impuestos, las solicitudes de beneficios sociales en un sitio web estatal, etc. Todas ellas son situaciones cada vez más habituales que, incluso, forman parte las diversas iniciativas de digitalización del Estado, o dicho de otro modo, de la profundización del gobierno electrónico.

Cualquier iniciativa que limite las actualizaciones de programas informáticos, o que persiga implementar vulnerabilidades mediante estas actualizaciones, puede generar consecuencias muy negativas en términos de seguridad y confianza de las personas. Por tanto, deben evitarse, corregirse en caso de que persistan esas limitaciones, y rechazarse abiertamente si no son subsanadas.

Ante estas situaciones, un primer paso para la protección de la seguridad digital de las personas es que los sitios web implementen obligatoriamente un protocolo de cifrado robusto, como el protocolo de transmisión segura de datos. Este protocolo permite que los datos que viajan por internet lo hagan de forma oculta, reduciendo significativamente su interceptación por un actor malicioso.[58] De esta forma, recomendamos a los Estados corregir malas prácticas que aún exigen a la ciudadanía acceder a servicios gubernamentales digitales a través de navegadores obsoletos y desactualizados (ej. Internet Explorer 10).[59]

Principio 8. Impulsar la participación multisectorial

Si bien todavía es predominante la idea de algunos gobiernos de que la seguridad digital debería estar bajo el ámbito de los Estados y trabajarse en estrecha colaboración con el

dades de seguridad vinculadas al sistema de votación electrónica de la Ciudad de Buenos Aires fue denunciado penalmente. Tras un proceso judicial de más de un año, que incluyó el allanamiento de todos sus dispositivos electrónicos, fue sobreseído a mediados de 2016. *Véase* Sobreseyeron al programador que reveló fallas en el sistema de voto por Boleta Única Electrónica (2016, 2 de agosto). *La Nación*. Disponible en http://www.lanacion.com.ar/1924088-sobreseyeron-alprogramador-que-revelo-fallas-en-el-sistema-de-boleta-unica-electronica

58 Para más información, *véase* Fundación Karisma. (s.f.). Navegación segura. *Genios de internet, 3*. Disponible en http://internetactiva.net/recursos/genios-de-internet-una-guia-para-mejorar-tu-seguridad-en-la-red/no-3-navegacion-segura/.

59 Microsoft. (2016). *Se ha dejado de ofrecer soporte para las versiones anteriores de Internet Explorer*. Disponible en https://www.microsoft.com/es-es/windowsforbusiness/end-of-ie-support.

sector privado, cada vez es más fuerte el argumento de que las políticas y medidas de seguridad digital deben construirse desde una aproximación multisectorial, es decir, con múltiples partes interesadas.

Así se ha expresado en el *Documento final de la reunión de alto nivel de la Asamblea General sobre el examen general de la aplicación de los resultados de la Cumbre Mundial sobre la Sociedad de la Información* (WSIS, por sus siglas en inglés), en donde se reiteró que "se debe promover y desarrollar una cultura global de ciberseguridad", para lo que "las medidas de ciberseguridad deben implementarse en cooperación con todas las partes interesadas".[60]

Además, desde hace varios años existen foros internacionales que han adoptado una aproximación multisectorial como, por ejemplo, la WSIS, la Conferencia Mundial del Ciberespacio (GCCS, por sus siglas en inglés), el Foro de Gobernanza de Internet (IGF, por sus siglas en inglés), la UIT, y grupos técnicos como el *Internet Engineering Task Force* (IETF).

A un nivel nacional, la instancia más destacable es el caso de Brasil y su Comité Gestor de Internet (CGI.br), que aunque ha estado bajo ataque en el último tiempo, es la organización multisectorial responsable de promover el desarrollo tecnológico de los servicios de internet y de difundir información con respecto a las últimas innovaciones y servicios disponibles en Brasil.[61]

La necesidad de colaborar e intercambiar información entre las múltiples partes interesadas cobra mayor relevancia si se tiene en cuenta la naturaleza misma del ciberespacio y de cómo las amenazas a la seguridad digital afectan a todo el ecosistema digital. Para atender de forma más efectiva estas amenazas, es necesario crear procesos participativos, abiertos, multisectoriales e inclusivos. Estos pueden incluir la construcción de políticas y medidas de seguridad digital entre quienes crean, supervisan, custodian, investigan y utilizan sistemas informáticos y tecnologías de la información; es decir, entre los gobiernos, el sector privado, la comunidad técnica, la academia y la sociedad civil.

Por todo lo anterior, se vuelve primordial establecer una comprensión común entre todas las partes interesadas acerca de las amenazas a la seguridad digital, y así poder tomar medidas más efectivas de protección de la información. También es necesario

60 Asamblea General de ONU. (2016, 1 de febrero). *WSIS+10 Outcome Document 2015.* A/RES/70/125, párrs. 50-52. Disponible en http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/70/125
61 Véase la nota de repudio de la *Colación brasilera por los derechos de la red* en https://direitosnarede.org.br/p/temers-government-attacks-cgi-br/.

un reconocimiento común de los papeles y responsabilidades de cada actor con el fin de prevenir y mitigar eficazmente las amenazas. Esa definición común debe ser lo suficientemente flexible para permitir que cada actor desempeñe sus funciones de acuerdo a las diferentes medidas de seguridad digital que se estén discutiendo.

Esto es especialmente crucial para la sociedad civil, sector conformado por una amplia diversidad de grupos de interés que trabajan de formas diferentes. En sus distintas facetas, la sociedad civil puede asumir un papel de experta, pero también puede simplemente expresar preocupaciones de la ciudadanía. Además, puede tomar el papel de veedora o fiscalizadora de las actuaciones públicas y/o privadas, y ofrecer evidencias que ayuden en la construcción de políticas.

La comunidad técnica, por su parte, puede cumplir un papel crítico de asesoramiento independiente sobre las posibles consecuencias de las decisiones de políticas públicas en seguridad digital, y la forma en la que las medidas propuestas podrían o no funcionar o impactar el ecosistema digital.[62] Por su parte, la academia puede aportar con investigaciones; estudios comparados; modelos teóricos, descriptivos, predictivos, etc; análisis desde diferentes perspectivas o escuelas teóricas, de discurso, de comportamientos de indicadores en el tiempo; propuestas de indicadores de evaluación, etc., que proveen insumos o material para informar los procesos de toma de decisiones. El sector privado, que incluye a las proveedoras de servicios de internet y al sector de tecnologías de la información, es crucial por su papel en la creación, manejo y mantenimiento de redes y tecnologías sujetas a amenazas.

Sin lugar a dudas, los gobiernos están en mejor condición de liderar los esfuerzos en torno a la seguridad digital, pero deben promover y asegurar procesos participativos, abiertos, multisectoriales e inclusivos.[63] Apostar por procesos que reúnan las características antes mencionadas permite tener mejores políticas, tendientes a garantizar el efectivo disfrute de los derechos humanos en entornos digitales, así como facilitar el desarrollo de normas y medidas para su implementación. Esto, a su vez, otorga mayor legitimidad y sostenibilidad a las mismas.

Un ejemplo puede encontrarse en la recién adoptada política de ciberseguridad chilena, resultado de un proceso que demostró el interés del Gobierno en construir un hoja de ruta, de manera participativa, abierta e inclusiva, y que atendiera los desafíos de la seguridad

62 IEEE. (2016, 25 de junio). *The Role of the Technical Community in Internet Policy.* Disponible en http://globalpolicy.ieee.org/wp-content/uploads/2017/06/IEEE17016.pdf.
63 Global Partner Digital. (2017). *Framework for Multistakeholder Cyber Policy Development*. Disponible en https://www.gp-digital.org/wp-content/uploads/2017/03/Framework-for-cyber-policymaking.pdf.

digital en los próximos años.[64] El comité gubernamental encargado de este proceso no solo abrió un proceso de consulta pública, sino que hizo invitación directa a diversos actores de la sociedad civil, las empresas, otros organismos públicos y la comunidad técnica. La consulta también estuvo acompañada por audiencias temáticas con las partes interesadas, en las que se atendieron, de manera transparente y participativa, posiciones de diversos actores vinculados a la materia.

La cooperación entre las diferentes partes es decisiva para comprender las amenazas digitales y llevar a cabo mejores evaluaciones de la efectividad de las acciones de cada actor en el ciberespacio. Ahí reside la importancia de incluir múltiples voces e intereses en la construcción e implementación de políticas o estrategias nacionales de seguridad digital. Es responsabilidad de los gobiernos garantizar que la participación sea amplia, diversa, inclusiva y efectiva.

Principio 9. Recoger e implementar experiencias y buenas prácticas

Cuando en este principio nos referimos a las evaluación de experiencias e implementación adaptada de buenas prácticas, es necesario reconocer el importante papel de liderazgo que juega el sector público tanto al mostrar sus fuertes compromisos para con el respeto de los derechos humanos en la implementación de políticas o estrategias nacionales de seguridad digital, como también en la transparencia y rendición de cuentas sobre su actuar. Esto establecerá el ejemplo para las otras partes interesadas, además de que mejorará la confianza al proporcionar una dirección clara a los actores del ecosistema digital de cada país.

Una política o estrategia nacional de seguridad digital que ponga en práctica lo antes mencionado, permitirá que en el futuro se tomen decisiones y medidas más fundamentadas y equilibradas para el beneficio socioeconómico de cada país. En ese proceso, además, es fundamental el intercambio de experiencias y buenas prácticas, pues permite tener una mejor preparación y reacción ante los riesgos digitales. Por tanto, con este principio buscamos incentivar a los Estados a que se den esos procesos de intercambio.

A nivel global existen ejemplos de alianzas y grupos que trabajan con la idea de compartir y documentar experiencias y buenas prácticas. El Foro Global de Ciberexperiencias (GFCE,

64 Viollier, P. (2017). *La participación en la elaboración de la política nacional de ciberseguridad: hacia un nuevo marco normativo en Chile*. Santiago, Chile: Derechos Digitales. Disponible en https://www.derechosdigitales.org/wp-content/uploads/ciberseguridad.pdf.

por sus siglas en inglés) es una plataforma que reúne país, organizaciones internacionales y empresas con el fin de “identificar políticas, prácticas e ideas exitosas y multiplicarlas a nivel global […] para desarrollar la capacidad cibernética” de sus miembros.[65]

Otro ejemplo se encuentra en la Directiva europea sobre la seguridad de las redes y los sistemas de información que, entre otras cosas, impulsa la colaboración de los miembros de la Unión Europea a través de la creación de “un grupo de cooperación para apoyar y facilitar la colaboración estratégica y el intercambio de información entre los Estados miembros”.[66] Más específicamente, esta directiva establece que su finalidad “es mejorar el funcionamiento del mercado interior mediante la creación de un clima de confianza y seguridad, [para ello,] los organismos de los Estados miembros deben poder cooperar eficazmente con los agentes económicos y han de estar estructurados en consecuencia”.[67] Así, reconoce las ventajas del intercambio y la colaboración como un medio para proponer soluciones globales a las cuestiones de seguridad digital.

También vale la pena destacar el informe de la OCDE sobre la gestión de riesgos para la prosperidad económica y social, que guía la elaboración de “una nueva generación de estrategias nacionales sobre la gestión del riesgo de la seguridad digital con el objetivo de optimizar los beneficios económicos y sociales que se esperan de un entorno digital abierto” (Traducción nuestra).[68] En ella se desarrollan principios y recomendaciones que pueden resumirse en la siguiente discusión.

Es necesario que todas las partes interesadas sepan los riesgos a la seguridad digital y cómo manejarlos desde una aproximación de derechos humanos. Eso implica que las partes asuman la responsabilidad de la gestión del riesgo dentro de sus capacidades y alcances, y según su propio papel en el ecosistema digital. Finalmente, esto requiere la cooperación de todas las partes interesadas para evitar la adopción de decisiones que impacten negativamente en el respeto por los derechos humanos, que sean tecnológicamente defectuosas o que impidan la innovación. Esa colaboración, sin duda, servirá para informar procesos o mecanismos internacionales y/o regionales creados o por crear de los que también recomendamos a los Estados formar parte.

---

65 *Véase* el sitio web del GFCE en https://www.thegfce.com/about.
66 European Commission (2016, 5 de julio). *The Directive on security of network and information systems* (NIS Directive). Disponible en https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive
67 Directiva No. 1148 del Parlamento Europeo y del Consejo (2016, 6 de julio). *Medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión*, párr. 31. Disponible en http://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32016L1148&from=EN
68 OECD. (2015). *Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document*. Paris, France: OECD Publishing. DOI http://dx.doi.org/10.1787/9789264245471-en.

A nivel nacional, por tanto, a instamos que se creen esos mecanismos y procesos de cooperación entre las diferentes partes interesadas que permitan tener decisiones más informadas y equilibradas.

Principio 10. Adoptar estándares abiertos de tecnología

El crecimiento del impacto y la frecuencia de los ataques digitales obliga a tener políticas, tecnologías y procedimientos adecuados y suficientemente flexibles para que permitan proteger el valor socioeconómico de internet. La flexibilidad de que hablamos también posibilita abordar nuevos fenómenos como lo son el creciente desarrollo de la internet de las cosas. Esto exige la implementación de enfoques abiertos, transparentes e inclusivos, especialmente en el desarrollo de estándares.

Los gobiernos –como propietarios, usuarios, administradores y/u operadores de sistemas de información y redes– podrían liderar con el ejemplo mediante la adopción de mejores prácticas, tecnologías e incluso requisitos legislativos. Las políticas o estrategias nacionales de seguridad digital podrían alentar el desarrollo y/o adopción de estos estándares abiertos para brindar soluciones de seguridad. En este sentido, es importante que los Estados muestren su compromiso con una internet abierta, descentralizada y neutral.

Lo anterior es especialmente importante si se considera, como lo apuntaron la comunidad técnica y el sector privado en una consulta realizada por la OCDE en 2012, que favorecer “requisitos unilaterales [por los gobiernos] para utilizar estándares o tecnologías locales, [u] obligaciones innecesarias o redundantes de documentación o certificaciones” puede generar un impacto negativo en la seguridad digital.[69] De hacerlo, se puede afectar el costo y limitar la funcionalidad de las tecnologías, así como restringir la innovación.

Por ello, instamos a los Estados a fomentar la adopción de estándares abiertos que aprueban organismos de desarrollo de estándares de internet como el *World Wide Web Consortium* (W3C), el *Institute of Electrical and Electronic Engineering Standard Association* (IEEE-SA) o el IETF. Las políticas o estrategias nacionales de seguridad digital, al final de cuentas, deben propender a una internet más segura, que esté respaldada por el desarrollo de componentes técnicos basados en modelos de estándares abiertos.

69 OECD. (2012). *Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy*, p. 49. Disponible en https://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf

Sobre los organismos el W3C, el IETF y el IEEE, podemos decir que han desarrollado un conjunto de estándares que pueden considerarse como la base de internet. En su conjunto, estos estándares también han sido un facilitador clave para el ejercicio de derechos humanos en internet. Veamos de qué manera son relevante en esta discusión.

El W3C trabaja para hacer que la web sea accesible para todas las persona a pesar de las diferencias culturales, educativas, capacidades, recursos y limitaciones físicas. El objetivo principal de este consorcio es desarrollar protocolos abiertos y directrices para aspectos clave de la web (ej. código HTML y CSS, guías de seguridad y privacidad, etc.).[70] Desde que se fundó en la década de los 90, el W3C ha publicado cientos de estándares –conocidas como recomendaciones–, que se han centrado en evitar la fragmentación de la web.[71] De esta manera, las recomendaciones de la W3C permiten acomodar la creciente diversidad de personas, hardware y software que convergen en el ecosistema digital.

La IEEE-AS es una organismo que desarrolla estándares globales en el campo de las ingenierías, incluyendo las áreas de tecnologías y seguridad de la información. Este organismo ha introducido una serie de estándares en seguridad digital desde hace algunos años. Algunos a destacar son un protocolo para proteger la integridad y confidencialidad de las comunicaciones a través de líneas telefónicas, ondas de radio, fibra óptica, etc.[72]; normas para la seguridad de los sistemas de control implementados por las compañías eléctricas[73]; y pautas para la comunicación segura a través de redes de acceso público, entre otros más que están en proceso de desarrollo.[74] Más recientemente, en mayo de 2017, publicó un informe en el que presenta un conjunto de medidas y buenas prácticas para la seguridad del tráfico de internet.[75] Como allí se menciona, este documento busca servir de guía para informar futuros desarrollos de estándares, certificaciones, políticas, legislaciones o certificaciones de productos.

El IETF, por su parte, es un organismo informal que estudia problemas operacionales y técnicos relacionados con internet, además de que desarrolla protocolos y soluciones a nivel de la arquitectura de internet. La mayor parte de su trabajo lo hace a través de varios

70 *Véase* la página web de Misión de la W3C en https://www.w3.org/Consortium/mission.
71 *Véase* la página web de Estándares de la W3C en https://www.w3.org/standards/.
72 *IEEE Std 1888.3-2013 - IEEE Standard for Ubiquitous Green Community Control Network: Security,* http://standards.ieee.org/findstds/standard/1888.3-2013.html.
73 *IEEE Std 1686-2013 (Revision of IEEE Std 1686-2007) - IEEE Standard for Intelligent Electronic Devices Cyber Security Capabilities,* http://standards.ieee.org/findstds/standard/1686-2013.html.
74 *IEEE Std C37.240-2014 - IEEE Standard Cybersecurity Requirements for Substation Automation, Protection, and Control Systems,* http://standards.ieee.org/findstds/standard/C37.240-2014.html.
75 IEEE. (2017). *Protecting Internet Traffic: Security Challenges and Solutions.* Disponible en https://internetinitiative.ieee.org/images/files/resources/white_papers/protecting_internet_traffic_may_2017.pdf.

grupos de trabajo, cada uno interesado en un tema particular de internet. Estos grupos suelen documentar su trabajo en una o más solicitudes de comentarios (RFC, por sus siglas en inglés), que a veces se convierten en estándares que ayudan a definir cómo funciona internet. Desde sus orígenes, este organismo ha mostrado una preocupación por la privacidad y la seguridad de la información, aunque más desde la parte técnica.[76] Sin embargo, desde hace un tiempo uno de sus grupos de trabajo está analizando el impacto de la arquitectura de internet en el ejercicio de derechos humanos. Para ello, trabaja en un documento en el que se muestra "la relación entre los protocolos y los derechos humanos" y propone "posibles pautas para proteger internet como un entorno propicio para los derechos humanos en el futuro desarrollo de protocolos".[77]

De otra parte, en cuanto al desarrollo de estándares nacionales de seguridad digital, hay que destacar el trabajo del *National Institute for Standards and Technology* (NIST) del Departamento de Comercio de los Estados Unidos, que surgió a principios de siglo XX con el fin de generar estándares en medición, normas y tecnologías.[78] Desde 2012, el NIST ha estado trabajando en la construcción de un marco de seguridad digital que trata de medir las capacidades de las instituciones para responder a ataques informáticos.[79] También ha resultado útil para la formulación de procesos de construcción de sistema de seguridad digital en organizaciones de distintos tipos.[80] Este esfuerzo representa una iniciativa importante para la estandarización de la privacidad y la seguridad en entornos digitales para actores individuales.

El NIST, sin lugar a duda, también es un buen ejemplo que muestra la apertura de sus grupos de trabajo. En ellos intervienen personas con diferentes experticia en la elaboración de marcos de acción y estándares. Aunque estos marcos no son necesariamente vinculantes, a veces terminan siéndolo cuando los tribunales analizan modelos de conducta para establecer responsabilidad por daños.

76 *Véase* Cath, C.J.N. & Floridi, L. (2017, 6 de febrero). *The Design of the Internet's Architecture by the Internet Engineering Task Force (IETF) and Human Rights*. Disponible en http://dx.doi.org/10.2139/ssrn.2912308; Aboba, B. et al. (2013). *Privacy Considerations for Internet Protocols. Internet Architecture Board.* Disponible en https://tools.ietf.org/pdf/rfc6973.pdf

77 Cath, C. & ten Oever, N. (2017). *Research into Human Rights Protocol Considerations.* Internet Research Task Force. Disponible en https://datatracker.ietf.org/doc/rfc8280/

78 NIST. (2012). *Smart Grid Advisory Committee Report*. Disponible en https://www.nist.gov/sites/default/files/documents/smartgrid/NIST_SGAC_Final_Recommendations_Report_3-05-12_with_Attachments.pdf.

79 *Véase* el marco de ciberseguridad desarrollado por el NIST en https://www.nist.gov/cyberframework.

80 NIST. (2014, 14 de febrero). *Framework for Improving Critical Infrastructure Cybersecurity*. Disponible en https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf

En suma, los estándares abiertos de seguridad digital son técnicas que intentan proteger el ciberespacio, reduciendo sus riesgos. Pueden expresarse en herramientas, políticas, medidas, enfoques, mejores prácticas y acciones, que deben ser consideradas y estudiadas por los Estados, en colaboración con las diferentes partes interesadas, a la hora de elaborar e implementar políticas o estrategias nacionales de seguridad digital. Están ahí para ser utilizadas y evitar la elaboración desde cero, pero con suficiente flexibilidad para ser adaptadas a los modelos de resigo de cada país o sector, y desarrollos más recientes como el internet de las cosas.


por los Derechos Civiles


PRIVACY
INTERNATIONAL


TE
DIC
TECNOLOGÍA &
COMUNIDAD


Fundación
Karisma